IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Regarding the application:

Title:	User selection of computer login	Examiner:	Cervetti, David Garcia
Number:	10/090,520	Art Unit:	2136
Priority:	April 26, 2001		

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

BRIEF FOR APPELLANT

This is an appeal from the Examiner's October 27, 2006 final rejection.

(I) REAL PARTY IN INTEREST

Gary Odom, appellant, is the real party in interest.

(II) RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences.

(III) STATUS OF CLAIMS

Appeal is sought for rejection of claims 27-49. Claims 1-26 have been canceled.

(IV) STATUS OF AMENDMENTS

An amended disclosure, compliant with 37 CFR 1.77, has been filed subsequent to final rejection.

(V) SUMMARY OF CLAIMED SUBJECT MATTER

In the summary below, citation of disclosure passages are noted by paragraph number, followed by figure number(s).

A transmission is user input via a device. [0033] A transmission may be made of multiple devices. [0034]; Figures 3, 4, 6

A signal is related data from a single transmission. Multiple signal types may emanate from a single transmission. [0035]; Figures 5, 6

A user creates a signature for subsequent authentication by first choosing the device or devices used among multiple devices. Preferably a user determines the input devices (transmissions) and signal types as well as the content of signals. Multiple devices may be used to create a signature. [0004], [0034], [0040], [0045], [0047], [0048]; Figures 9, 10, 11

Multiple discontiguous data blocks (keys) in a one or more files are used for authentication. [0006], [0059]-[0062]; Figure 11. A key may have all the data necessary for authentication, that is, be integral, or may be strung together by reference, as in a linked list. [0062]-[0070], [0073]; Figures 12, 16-19

Incremental authentication of a signature commences by accumulating possible keys, then discarding keys that don't match as additional signature data portions are input. Such an authentication fails if input continues and there are no more keys to match against, or succeeds by matching the last key in a chain with it corresponding user input portion [0087]-[0096]; Figures 12, 16-19

A user may determine a degree of inexactness, or tolerance level, for authentication matching. [0041]

Submission of a signature for authentication may terminated passively, including the user determining when passive termination is to occur. [0042], [0043], [0046]; Figure 8, 9

(VI) GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The following are the grounds of rejection to be reviewed on appeal: (1) rejection of claim 42 under 35 U.S.C. §112, ¶ 2; (2) rejection of claims 27-49 under 35 U.S.C. §102(b) as being anticipated by USPN 5,229,764 (Matchett); (3) rejection of claims 27-32, 35-39, and 41 under

U.S.C. §102(b) as being anticipated by USPN 6,052,468 (Hillhouse); (4) rejection of claims under U.S.C. §103(a) as being anticipated by USPN 5,229,764 (Matchett) for claim 49, and USPN 6,052,468 (Hillhouse) for claims 33-34, 40.

(VII) ARGUMENT

REJECTION OF CLAIM 42 UNDER 35 U.S.C. §112 ¶ 2

MPEP 2171 recites the following regarding §112 ¶ 2 rejections -

> The second requirement… is evaluated in the context of whether the claim is definite - i.e., whether the scope of the claim is clear to a hypothetical person possessing the ordinary level of skill in the pertinent art.
>
> [A]nother essential purpose of patent examination is to determine whether or not the claims are precise, clear, correct, and unambiguous. The uncertainties of claim scope should be removed, as much as possible, during the examination process.

Examiner complained of the claim as "generally indefinite," "replete with grammatical and idiomatic errors, e.g. ""wherein said signature divisible into portions, wherein said keys associating portions sequentially either integrally or by reference" it is not clear what this is supposed to mean."

There was nothing idiomatic about the examiner-cited phrases within the claim, other than being in the peculiar prose that constitutes patent claims in general, and, respectfully, the grammar is passable at worst; the claim may have more easily read "signature is divisible," but that in no way affects interpretation of the scope of the claim. Most importantly, as demonstrated below, there is no issue of the metes and bounds of claim scope, which is the basis for sustaining a §112 ¶ 2 rejection.

Respectfully, if one requires substance as a basis for rejection, Examiner's holistic damning of claim 42 is reduced to his not understanding two limitations: "wherein said signature divisible into portions, wherein said keys associating portions sequentially either integrally or by reference."

With all due respect, any native English speaker with a meager background in patent law should have little difficulty discerning the definite and specific limitations of claim 42. Yes, the claim language is compact, and has definitional precision in being so; there should be nothing wrong with that; quite the contrary, the claim is tightly written. Most importantly, any one with modest software programming skill and a good grasp of English should easily understand the scope being claimed.

Respectfully, if the examiner was dissatisfied with the claim language, he had a chance to adhere to MPEP 2171 by working with applicant by better explaining himself in rejection and not sending a final office action.

To demonstrate that the claims are allowable as definite, appellant herein recites each limitation of the claim with a translation in plainer, and vernacular, English, certainly within the "ordinary level of skill in the pertinent art."

42. A computer-implemented method for incrementally authenticating a signature while receiving user input comprising [translation: computer software accepts user input of an identifier, i.e. a "signature", while authenticating user input portion by portion (incrementally)]:

receiving a first portion of user input data; [translation: the software gets (receives into memory) a first portion of user input data]

accumulating keys based upon matching correspondingly key data to said first portion of user input data, [translation: software accumulates a bunch (or set) of keys by matching the first portion of user input data with data in previously stored keys; "matching correspondingly" means matching the first user input data portion to a corresponding portion of stored key data]

wherein a key comprises at least in part a portion of a previously stored signature, [translation: a key has a portion of a stored signature]

wherein said signature divisible into portions, [translation: a signature can be split (is divisible) into portions]

wherein said keys associating portions sequentially, either integrally or by reference; [translation: keys string together (associate) sequentially (that is, in the order of input), the portions being strung together either by be included in a key (integrally) or by using pointers to

other keys strung together in a chain (by reference); pointers are a hoary software technique, such as with linked lists]

subsequently, iteratively receiving a plurality of portions of user input data and performing a corresponding authentication step for each portion, [translation: next (subsequently), repeatedly (iteratively) receive further user input portions, and perform a corresponding authentication step for each user input portion]

wherein, upon receiving each subsequent portion after said first portion, discarding from further processing previously accumulated keys based upon failure in matching respective key data to said user input data portion; and [translation: for each newly received input portion, discard the previously gotten key chains if they don't match the new input portion]

whereby continuing said iterative process until completing authentication by matching said last key to corresponding said user input data portion, or by process of elimination determining authentication impossible. [translation: repeat the process until authentication is completed by key matching, or you run out of keys because none of them match.]

To prove the point that the claim is quite precise in its scope, here is the whole claim translated into high-school level English, albeit with less precision than the actual claim language, where the "skilled in the art" high schooler has programmed a bit (enough to know basic data structures):

> Software accumulates a bunch (or set) of keys by matching the first portion of user input data with data in previously stored keys - match the first user input data portion to a corresponding portion of stored key data; where a key has a portion of a stored signature; where a signature can be split into portions; keys string together in the order of input, the portions being strung together either by be included in a key or by using pointers to other keys strung together in a chain; next, repeatedly receive further user input portions, and perform a corresponding authentication step for each user input portion; for each newly received input portion, discard the previously gotten key chains if they don't match the new input portion; repeat the process until authentication is completed by key matching, or you run out of keys because none of them match.

REJECTION OF CLAIMS 27-49 UNDER 35 U.S.C. §102(B) AS BEING ANTICIPATED BY USPN 5,229,764 (MATCHETT)

Examiner rejected appellant's arguments describing that Matchett did not anticipate the claims herein. Appellant therefore appeals those rejections with the following arguments, as well as examiner's newer rejections of claims 42-49.

Dependent claims not explicitly argued herein depend upon the novel limitations of their respective independent claims as reasons for allowance.

CLAIM 27

Matchett failed to anticipate two novel limitations of claim 27: user device selection, and recording multiple signal types.

Claim 27: "creating a signature" using "at least one user-selected device among a plurality of selectable user input devices." In plain English, the claim states that a user selects the device(s) for creating a signature, among multiple devices to choose from. Matchett's disclosure in [5:54-63], and elsewhere, is of a user selecting to "program" a device required by the system to create her signature; the user does not get to select the device.

Examiner stated in his final office action: "Examiner points Applicant to the specification where it appears that the signature is generated (or may be) using a combination of inputs from more than one input device (pp. 6-7)." But, respectfully, examiner's statement is irrelevant, as it provides nothing as a basis for rejection of the claim, and is not even part of the claim.

Examiner stated in his final office action: "(1) Regarding Applicant's arguments, they attempt to differentiate between users selecting, as oppose to an administrator or manager or a programmed system (see Remarks, claim 27). (2) Matchett clearly lets users select from a plurality of input devices to authenticate. (3) Furthermore, the fact that the claims state from at least one, perfectly read on Matchett authenticating a user through a biometric reader (voice input data, column 6)."

(1) User selection contemporaneous with signature input is patentably different than a static system configured by an administrator, where the user does not get to make a choice in creating a signature at the time of creating the signature. This is a crucial aspect of the claimed

invention, as it vastly expands the combinations and permutations for signature types. In discussing this feature, the summary noted in [0004]: "This makes submission theft more difficult and less likely." With all due respect, examiner's statement in this regard indicates that the examiner utterly failed to comprehend the nature of the invention.

(2) Examiner's assertion that "Matchett clearly lets users select from a plurality of input devices to authenticate" is unsupported. First of all, with all due respect, examiner makes no sense, as a user does not choose a device "to authenticate." As claimed, a user chooses a device to create a signature. Authentication is not part of the claimed process. Second, and most important, with all due respect, examiner is making nothing less than a wild assertion without substantiation that Matchett anticipates the claimed user device selection. Examiner did not, and can not, specifically point to a passage in Matchett anticipating this limitation.

(3) Again, with all due respect, examiner is inscrutable, and his rejection indecipherable. How does "at least one" with regard to the claimed "user-selected device" provide Matchett with anticipation? Matchett [6:34-42] mentions using multiple biometric devices, but nowhere does Matchett indicate that the user chooses which devices are to be used.

Further, Matchett also failed to anticipate "at least one user-selectable input device affords recording a plurality of signal types." Examiner never commented on this, though this was presented to him in reply to examiner's non-final office action dated July 19, 2006.

CLAIMS 28, 36, 42, 45

Not only is there no indication in Matchett that multiple devices were used to create a single signature as claimed, Matchett taught away from creating a single signature using multiple devices. Matchett in Examiner-cited [9:10-68] disclosed user input into multiple biometric authentication devices. Describing Figure 4, Matchett disclosed authentication "data is stored in the respective one of the digital storage devices 418-426…" [9:31-32] Those data are then compared to "reference data." Thus, Matchett created separate signatures for each device; Matchett gave no indication otherwise. Examiner's rejection of claim 45 based on this passage indicates that Matchett taught away from claims 28, 36, 42, 45, & 47, which claim a single signature, not Matchett's multiple signatures.

CLAIM 29

Nowhere in Matchett, including Examiner-cited [5:15-6:68], is there anticipation of the claimed limitations in 29, either of user selection of signal type, or multiple signal types associated with a user input device.

CLAIM 30

Claim 30 excludes biometrics, which are not "user-controllable in duration" as claimed. A biometric device automatically stops reading when it has gathered sufficient data. Matchett therefore did not anticipate passive termination as claimed, where "signal input… is user-controllable in duration".

CLAIM 32

Examiner was correct that Matchett [10:10-35] disclosed threshold tolerances, and was correct in stating "is mute regarding who/what provides the threshold…" Examiner then stretched the point in writing that Matchett "suggests that the user may supply it." Matchett made no such suggestion. With all due respect, in his enthusiasm, Examiner has applied impermissible hindsight. Consistent with Matchett's description, the system is programmed to behave within certain parameters; a system over which the user had no disclosed control for adjustment. Claim 32, by contrast, has the novel limitation of "user-designated tolerance."

CLAIM 35

Please see above arguments for claim 27 with regard to user selection. Claim 35 specifies: (1) "user selection of … [a] signal type"; and (2) "user-selected input device." Matchett offered no such user selection, either of input device(s), or the signal types for use in creating a signature. Examiner had cited Matchett [6:1-68], but no such anticipation exists in that column, or anywhere else in Matchett.

Also, as with claim 27, Matchett lacked anticipation of a device being able to record multiple signal types from the claimed "user-selectable input device" which Matchett did not anticipate.

CLAIM 37

With all due respect, Matchett stated nothing, including Examiner-cited [4:30-5:15], about recording signature signals of multiple types prior to receiving user selection of the type(s) to use, as per claim 37.

CLAIM 38

Matchett failed to anticipate whatsoever creating a signature "wherein at least one said signal type comprises input from a plurality of devices," particularly Examiner-cited [6:1-68].

CLAIM 41

Matchett had nothing to say about recording a signature of "a plurality of user-selected signal types," including Examiner-cited [6:1-68].

CLAIM 42

Examiner's citation of Matchett [11:30-68] did not disclose anticipation of the claimed process as a whole. In a conceded point of relevance, Matchett disclosed the limitation of monitoring for unprompted input at [11:43-46]. Matchett did not anticipate accumulating keys based "upon receiving a first portion of … user input" as claimed. Matchett did not anticipate thereupon "discarding from further processing previously accumulated keys." In short, Matchett did not discloses the claimed key accumulation, followed by process-of-elimination, for authentication.

Please see the foregoing argument with regard to claim 28, et cetera, that Matchet taught away from creating a single signature using multiple devices as claimed in 42.

CLAIM 43

Claim 43 relies upon the novel limitations of independent claim 42.

CLAIM 44

Matchett never even mentioned the concept of key-based authentication as claimed in 42, let alone accessing keys by reference as claimed in 44, withstanding Examiner-cited [6:1-68].

CLAIM 46

While retaining the claim limitation of "a user-selected input device," like claim 27, claim 46 goes to structuring storage of signature data. Matchett's failure to anticipate "a user-selected input device" has been chronicled foregoing in remarks for claim 27; please see those remarks.

Also as argued foregoing with regard to claim 29, Matchett failed to anticipate "at least two signals types… associated with at least one single input device."

Examiner had cited [9:10-68], but nowhere does Matchett anticipate the claimed "partitioning… signature data by transmission type and by signal type."

Respectfully, examiner's citations of Matchett [6:1-68] and [9:10-68] failed to disclose what examiner asserted.

CLAIM 47

Matchett made no mention of the claimed limitation "partitioning… [a] signature into portions by signal type, such that at least one portion references another portion of said signature," nor did examiner address this novel limitation in his office action.

Please see the foregoing argument with regard to claim 28, et cetera, that Matchet taught away from creating a single signature using multiple devices as claimed in 47.

CLAIM 48

As argued with regard to claim 27, Matchett did not anticipate user device selection as claimed.

Nor did Matchett anticipate by any mention, as claimed, "recording user input of a plurality of signal types."

Nor did Matchett anticipate by any mention, as claimed, "receiving user selection among those signal types recorded."

Nor did Matchett anticipate by any mention, as claimed, "receiving user selection of at least one less signal type than recorded for said device."

Nor did Matchett anticipate by any mention, as claimed, "creating a signature comprising at least in part… user-selected signal types."

Respectfully, examiner's citation of Matchett columns 5-6 did not disclose what examiner asserted. With all due respect, this is consistent with examiner, throughout his office actions, of making reckless assertions of prior art anticipation that were not substantiated within the prior art reference itself.

REJECTION OF CLAIMS 27-32, 35-39, AND 41 UNDER U.S.C. §102(B) AS BEING ANTICIPATED BY USPN 6,052,468 (HILLHOUSE)

Hillhouse disclosed user selection of one of three "authentication method[s]": 1) a biometric authentication method; 2) a password; or 3) a key; nothing more

The most relevant section of the Hillhouse disclosure to the rejected claims is [7:2-14] (emphasis added):

> [A] user selects an authentication method in the form of a biometric authentication method such as a fingerprint, a voiceprint, facial features, a palm print, a retinal scan, and so forth; a password; or a key. The authentication method is selected from a plurality of available authentication methods. The user is authenticated according to the selected method and the secured cryptographic key is secured according to that method. The twice-secured cryptographic key is stored in the key data file with data relating to the selected authorisation methods and an order of the securing operations. This allows for multiple user authentication based protection of key data files. [7:2-14]

Hillhouse was redundant in other passages, such as examiner-cited [7:28-52], and [8:1-67], but no additional germane information is extant. If in any doubt, please confirm this by careful reading of Hillhouse.

With all due respect, examiner repeatedly asserted anticipation in Hillhouse where none existed. This is readily verified by a more careful reading of Hillhouse than examiner bothered with.

CLAIM 27

There is no evidence that Hillhouse had anticipation of the claim 27 limitation that "at least one user-selectable input device affords recording a plurality of signal types."

Further, Hillhouse did not anticipate, as claimed, a "user-selected device among a plurality of selectable user input devices." Hillhouse stated that "a user selects an authentication method in the form of a biometric authentication method…; a password; or a key." Hillhouse's passage about biometric authentication method mentioned different exemplary devices, which is different than suggesting that the user had a choice of devices for authentication. The choice of methods for a user that Hillhouse anticipated were between biometric authentication using a single biometric device, for which there is no indication that the user had a choice of, or a password, or a key. Hillhouse said: a user chooses biometric, password, or key. Hillhouse simply gave examples of biometric devices. Hillhouse never suggested that a user would be able to select among different devices for authentication. Please read Hillhouse carefully and you too will see that what appellant states herein is accurate. Hillhouse makes essentially the same quote at [6:27-32], [7:2-8] and [8:3-7]; the user choice is method, not device. Read Hillhouse in its entirety in context, and you will see that Hillhouse user selection is among authentication methods (biometric device, password, or key), not devices as claimed.

CLAIM 35, 29

There is no evidence that Hillhouse had anticipation of the limitation in claims 35 and 29 of "receiving user selection of at least one signal type among a plurality of selectable signal types." More basically, Hillhouse did not disclose that an input device might record multiple user-selectable signal types as claimed.

CLAIMS 28, 36

Hillhouse had no anticipation of the claim 28 limitation of recording signals from multiple devices. Hillhouse only suggested the "a user selects an authentication method in the form of a biometric authentication method such as a fingerprint, a voiceprint, facial features, a palm print, a retinal scan, and so forth; a password; or a key." There was no suggestion of using multiple devices for the selected authentication method.

CLAIM 30

Hillhouse never suggested a creating a signature from "signal input that is user-controllable in duration." Examiner's citation of Hillhouse [8:1-67] yields no such anticipation.

CLAIMS 31, 39

Examiner had cited Hillhouse [8:1-67], but there is no evidence of Hillhouse having anticipated accepting authentication by "comparison within a predetermined degree of inexactness."

CLAIM 32

Examiner had cited Hillhouse [8:1-43], but there is no evidence of Hillhouse having anticipated the further limitation from claim 31 regarding inexactness matching of "user-designated tolerance."

CLAIM 37

Examiner had cited Hillhouse [8:1-67], but Hillhouse never suggested as claimed that "recording precedes [] receiving signal type selection," particularly considering that Hillhouse never anticipated the claim 35 limitation of recording multiple user-selectable signal types from an input device.

CLAIM 38

Examiner had cited Hillhouse [8:1-67], but there is no evidence of Hillhouse having anticipated a signal type from multiple device input.

CLAIM 41

There is no evidence that Hillhouse had anticipation of the claim 41 limitation of "recording [] a plurality of user-selected signal types."

REJECTION OF CLAIMS UNDER U.S.C. §103(A) AS BEING ANTICIPATED BY USPN 5,229,764 (MATCHETT) & USPN 6,052,468 (HILLHOUSE)

Dependent claims 33-34, 40, and 49 rely upon the novel limitations of their respective independent claims for reasons for allowance.

Appellant does not request an oral hearing.

The fee per 37 C.F.R. § 1.17 (c) for filing this appeal brief is included in electronic filing.

Thank you.

Respectfully submitted,

Gary Odom

123 NW 12th Avenue, #1545, Portland, OR 97209

telephone: (206) 529-5146 fax: (775) 942-8525
date: December 16, 2006

(VIII) CLAIMS APPENDIX

1-26. (canceled)

27. (previously presented) A computer-implemented method for creating a signature for subsequent authentication comprising:

indicating to a user commencement of signature input recording;

recording user input signals by type from at least one user-selected device among a plurality of selectable user input devices,

wherein a signal comprises a set of related software-recognizable data of the same type received from at least one input device, and

wherein at least one user-selectable input device affords recording a plurality of signal types, and

wherein a signal type comprises a category, among a plurality of possible categories, of measurable variable input associated with at least one user-selectable input device;

terminating said recording;

creating a signature based at least in part upon said recording; and

storing said signature.

28. (previously presented) The method according to claim 27, wherein said recording comprises signals from a plurality of user-selected devices.

29. (previously presented) The method according to claim 27, further comprising receiving user selection of at least one signal type from a plurality of signal types associated with at least one user input device.

30. (previously presented) The method according to claim 27, further comprising passively terminating authentication comparison of a subsequent signature submission to said recording,

thereby authenticating said subsequent signature; and

wherein said signature comprises at least in part signal input that is user-controllable in duration.

31. (previously presented) The method according to claim 27, further comprising:

comparing a subsequent signature submission to said recording,

and accepting said comparison within a predetermined degree of inexactness,

thereby authenticating said subsequent signature.

32. (previously presented) The method according to claim 31, wherein said predetermined degree comprises a user-designated tolerance.

33. (previously presented) The method according to claim 27, further comprising presenting at least a portion of said recording to said user for editing,

wherein said recording does not entirely comprise text-character codes.

34. (previously presented) The method according to claim 27, further comprising editing said recording,

wherein said signature is not entirely comprised of text-character codes.

35. (previously presented) A computer-implemented method for creating a signature for subsequent authentication comprising:

receiving user selection of at least one signal type among a plurality of selectable signal types;

recording input data of at least one signal type from at least one user-selected input device among a plurality of selectable user input devices,

wherein a signal type comprises a category, among a plurality of possible categories, of measurable variable input associated with at least one user-selectable input device,

and wherein at least one user-selectable input device affords recording a plurality of signal types; and

creating a signature comprising at least in part at least a portion of said input data of said user-selected signal types; and

storing said signature.

36. (previously presented) The method according to claim 35, wherein said recording comprises a plurality of user-selected devices.

37. (previously presented) The method according to claim 35, such that said recording precedes said receiving signal type selection.

38. (previously presented) The method according to claim 35, wherein at least one said signal type comprises input from a plurality of devices.

39. (previously presented) The method according to claim 35, further comprising:

comparing a subsequent signature submission to said recording,

and accepting said comparison within a designated tolerance of inexactness,

thereby authenticating said subsequent signature.

40. (previously presented) The method according to claim 35, further comprising editing said recording,

wherein said signature is not entirely comprised of text-character codes.

41. (previously presented) The method according to claim 35, wherein said recording comprises a plurality of user-selected signal types.

42. (previously presented) A computer-implemented method for incrementally authenticating a signature while receiving user input comprising:

receiving a first portion of user input data;

accumulating keys based upon matching correspondingly key data to said first portion of user input data,

wherein a key comprises at least in part a portion of a previously stored signature,

wherein said signature divisible into portions,

wherein said keys associating portions sequentially, either integrally or by reference;

subsequently, iteratively receiving a plurality of portions of user input data and performing a corresponding authentication step for each portion,

wherein, upon receiving each subsequent portion after said first portion, discarding from further processing previously accumulated keys based upon failure in matching respective key data to said user input data portion; and

whereby continuing said iterative process until completing authentication by matching said last key to corresponding said user input data portion, or by process of elimination determining authentication impossible.

43. (previously presented) The method according to claim 42, wherein accepting said match within a designated tolerance of inexactness.

44. (previously presented) The method according to claim 42, wherein accessing at least one key by reference from another key.

45. (previously presented) The method according to claim 42, wherein said first portion comprises input from a plurality of devices.

46. (previously presented) A computer-implemented method for storing the signatures of a plurality of users comprising:

recording a plurality of signatures comprising data of a plurality of transmission types and signal types,

wherein a transmission type comprises indicia of a user-selected input device among a plurality of user-selectable devices,

wherein a signal type comprises a category, among a plurality of possible categories, of measurable variable input associated with at least one user input device, and

wherein at least two signals types are associated with at least one single input device; and

partitioning said signature data by transmission type and by signal type.

47. (previously presented) The method according to claim 46, further comprising storing a signature at least in part by partitioning said signature into portions by signal type,

such that at least one portion references another portion of said signature.

48. (previously presented) A computer-implemented method for creating a signature comprising:

recording user input of a plurality of signal types from at least one user-selected device among a plurality of user-selectable devices,

wherein a signal type comprises a category, among a plurality of possible categories, of measurable variable input associated with at least one user input device;

receiving user selection among those signal types recorded,

whereby receiving user selection of at least one less signal type than recorded for said device;

creating a signature comprising at least in part said user-selected signal types.

49. (previously presented) The method according to claim 48, further comprising receiving user indication to edit said signature,

wherein said signature is not entirely comprised of text-character codes.

(IX) EVIDENCE APPENDIX

None. Examiner entered no evidence relied upon.

(X) RELATED PROCEEDINGS APPENDIX

None.